



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,325	03/16/2001	Leo J. Campbell	08049.0002	5367
22852	7590	08/24/2006	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/809,325	Applicant(s) CAMPBELL ET AL.	
	Examiner Thanhnga B. Truong	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 6/1/06 (RCE).
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-92 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-92 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Truong
 AU 2135

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 1, 2006 has been entered. Claims 1-92 are pending. At this time, claims 1-92 are rejected with new citations from French et al's reference.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-4, 6-8, 10-11, 29-35, 43-46, 48-50, 52-53, 71-77, 85, 87, 89, and 91 are rejected under 35 U.S.C. 102(e) as being anticipated by French et al (US 6,282,658 B2).

a. ***Referring to claim 1:***

i. French teaches a method for issuing a digital certificate to a user having an electronic account on a network, comprising the steps of:

(1) receiving a request for a digital certificate for the user having the electronic account [**i.e., once the authentication process has been satisfied, the invention may generate a digital certificate recording authentication levels and other information related to the user. The digital certificate can then**

be presented in future transactions to avoid the need to re-authenticate the user for each new transaction event. (column 2, lines 62-67));

(2) sending an identification verification form to a physical address of the use [i.e. Figure 42 illustrates an offline remote authentication embodiment of the invention, in which some processing including delivery of a validated ID is conducted using ordinary mail (column 19, lines 32-35));

(3) receiving the identification verification form from the user in person at a proofing workstation [i.e., first, standard field checks preferably occur at client 110, where and when the requested data is collected, to ensure that all required data is present and all provided data is in the proper format and meets minimum requirements. Completing this processing at client 110 minimizes the number of requests that must be terminated at this early point in the authentication process due to formally incorrect data. This is particularly important when the user is not present at the time of authentication, such as when requests are submitted in batch form rather than interactively. In general, the standard field checks make sure that an expected range or format of characters are input by the user, appropriate to individual queries and data types (column 8, line 61 through column 9, line 6)];

(4) verifying the identity of the user in person using the identification verification form at the proofing workstation [i.e., in the event the user will be paying for a product or service with a credit card, authentication process 10 may invoke credit card verification at this point. In this case, checks may be executed against a credit card database. These checks may include ensuring that the available credit line is sufficient to make the purchase, ensuring that the billing address for the credit card in the database matches the submitted address, and ensuring that the credit card is not stolen. Databases presenting this sort of information are commercially available (column 11, lines 17-26). In addition, referring to Figure 1, Preprocessing step 26 may thus include a set of validation checks including standard field checks, social security number validation, address validation, area code validation, and driver's license validation and other

preliminary data verification (column 8, lines 50-55). Furthermore, responses, or actions, for each of the possible address-related status codes or error codes in error code matrix 156 (illustrated in Figures 9-11) are provided as output during the preprocessing step 26. The user is preferably given only one additional attempt to correct each address that has been rejected by address validation. If the address cannot be corrected after a total of two attempts, the request proceeds as designated in the response matrix 154 illustrated in Figures 9-11 (column 10, lines 28-36)];

(5) when the identify of the user has been verified, generating the digital certificate by a certificate authority for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and linking the digital certificate to the electronic account of the user [i.e., referring to Figure 1, the user inputs that first level information via a keyboard, mouse, voice digitizer or other suitable input mechanism at step 16 Step 18 identifies that the user has completed first level information input. Step 20 transmits the input. The transaction record 112 is initialized at step 22. Step 24 performs an association check on the information input by the user. According French's invention, a user who wants to access information or process a transaction over a network is prompted to submit information to authentication process 10 through client 110. Authentication process 10 invokes the preprocessing step 26, in which the user is prompted to supply a first type of user identification information. The first type of user identification information preferably comprises wallet-type information such as name, address, phone number, social security number, driver's license number and other common personal information (column 6, lines 15-24). In addition, authentication process 10 matches, at step 32, the first type of information input by the user with information received from one or more separate data sources. Authentication process 10 also determines whether a request for information has been repeated more than a predetermined number of times at step 42. As illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or

Art Unit: 2135

password information to generate and store digital certificate 902. The digital certificate 902 contains a set of fields including user identification, a digital certificate serial number, an expiration period, as well as information related to the issuer of the digital certificate and fingerprint data for the digital certificate (column 16, lines 12-20)].

b. Referring to claim 2:

i. French further teaches:

(1) storing a reference to the digital certificate in a certificate directory at the certificate authority [i.e., as illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or password information to generate and store digital certificate 902. The digital certificate 902 contains a set of fields including user identification, a digital certificate serial number, an expiration period, as well as information related to the issuer of the digital certificate and fingerprint data for the digital certificate (column 16, lines 12-20)].

c. Referring to claim 3:

i. French further teaches:

(1) wherein the certificate authority includes a proofing server [i.e., referring to Figure 12, element 120 is an authentication/proofing server].

d. Referring to claim 4:

i. French further teaches:

(1) wherein the certificate authority further includes the proofing workstation [i.e., referring to Figure 12, element 140 is a computer and/or workstation. Furthermore, Figure 12 also shows one or more resources 140 which are accessible to application server 130. These may include, for example, databases, other computers, electronic memory, CD ROMs, RAID storage, tape or other archival storage, routers, terminals, and other peripherals and resources (column 6, lines 10-14)].

e. Referring to claims 6-8, 11:

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

f. Referring to claim 10:

i. French further teaches:

(1) wherein the digital certificate includes a public key for authenticating the digital certificate [i.e., **the biometric data may be used as input fields or records in the preprocessing, first or second authentication level stages. Alternatively, biometric data may be used as a key to unlock and release a digital certificate 902 issued to the user, to be stored on client 110 or otherwise (column 12, lines 59-63)]**].

g. Referring to claim 29:

i. French further teaches:

(1) receiving, at a proofing workstation, user information for the user with the electronic account, including an identification verification form previously sent to a physical address of the user [i.e., **first, standard field checks preferably occur at client 110, where and when the requested data is collected, to ensure that all required data is present and all provided data is in the proper format and meets minimum requirements. Completing this processing at client 110 minimizes the number of requests that must be terminated at this early point in the authentication process due to formally incorrect data. This is particularly important when the user is not present at the time of authentication, such as when requests are submitted in batch form rather than interactively. In general, the standard field checks make sure that an expected range or format of characters are input by the user, appropriate to individual queries and data types (column 8, line 61 through column 9, line 6). In addition, referring to Figure 13, the transaction record 112 (illustrated in Figures 13-16) initialized in step 22 is used throughout the authentication process 10 to keep track of user input and authentication results (column 14, lines 11-14). Furthermore, see column 19, lines 56-67 through column 20, lines 1-11 for relationship between electronic account and physical address]**]; verifying at the proofing workstation, identification

information from the user in person at the proofing workstation based on the identification verification form [i.e., in the event the user will be paying for a product or service with a credit card, authentication process 10 may invoke credit card verification at this point. In this case, checks may be executed against a credit card database. These checks may include ensuring that the available credit line is sufficient to make the purchase, ensuring that the billing address for the credit card in the database matches the submitted address, and ensuring that the credit card is not stolen. Databases presenting this sort of information are commercially available (column 11, lines 17-26). In addition, referring to Figure 1, Preprocessing step 26 may thus include a set of validation checks including standard field checks, social security number validation, address validation, area code validation, and driver's license validation and other preliminary data verification (column 8, lines 50-55). Furthermore, responses, or actions, for each of the possible address-related status codes or error codes in error code matrix 156 (illustrated in Figures 9-11) are provided as output during the preprocessing step 26. The user is preferably given only one additional attempt to correct each address that has been rejected by address validation. If the address cannot be corrected after a total of two attempts, the request proceeds as designated in the response matrix 154 illustrated in Figures 9-11 (column 10, lines 28-36)]; matching, at the proofing workstation, the user information to the identification information [i.e., referring to Figure 1, the user inputs that first level information via a keyboard, mouse, voice digitizer or other suitable input mechanism at step 16 Step 18 identifies that the user has completed first level information input. Step 20 transmits the input. The transaction record 112 is initialized at step 22. Step 24 performs an association check on the information input by the user. According French's invention, a user who wants to access information or process a transaction over a network is prompted to submit information to authentication process 10 through client 110. Authentication process 10 invokes the preprocessing step 26, in which the user is prompted to supply a first type of user identification information. The first type of user identification information

Art Unit: 2135

preferably comprises wallet-type information such as name, address, phone number, social security number, driver's license number and other common personal information (column 6, lines 15-24). In addition, authentication process 10 matches, at step 32, the first type of information input by the user with information received from one or more separate data sources. Authentication process 10 also determines whether a request for information has been repeated more than a predetermined number of times at step 42. As illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or password information to generate and store digital certificate 902. The digital certificate 902 contains a set of fields including user identification, a digital certificate serial number, an expiration period, as well as information related to the issuer of the digital certificate and fingerprint data for the digital certificate (column 16, lines 12-20)]; and

(2) sending by the proofing workstation to a proofing server, an identification verification from, when the user information has been matched to the identification information received from the user in person [i.e. referring to Figure 1, Preprocessing step 26 may thus include a set of validation checks including standard field checks, social security number validation, address validation, area code validation, and driver's license validation and other preliminary data verification (column 8, lines 50-55). Furthermore, responses, or actions, for each of the possible address-related status codes or error codes in error code matrix 156 (illustrated in Figures 9-11) are provided as output during the preprocessing step 26. The user is preferably given only one additional attempt to correct each address that has been rejected by address validation. If the address cannot be corrected after a total of two attempts, the request proceeds as designated in the response matrix 154 illustrated in Figures 9-11. The response matrix 154 may be located on authentication server 120, in authorization database 152 or elsewhere and serve to associate messages with test results and transaction records during the address portion of preprocessing step 26, concurrently with overall application processing. In other words, the

Art Unit: 2135

response matrix 154 sends messages to client 110 based upon specific verification tests or based upon the current status of the transaction record 112. For example, the message may prompt the user to verify that data which was input is correct or a message to direct the user to call customer service for manual intervention. The response matrix 154 is preferably parameter driven, so that appropriate messages can be associated with particular events (column 10, lines 28-50)].

h. Referring to claim 30:

i. French further teaches:

(1) receiving payment from the user at the proofing workstation [i.e., Table 2 shows the monthly payment amount appearing in the description column which provides by the users (column 8, lines 49)].

i. Referring to claim 31:

i. French further teaches:

(1) wherein the payment is received via credit card [i.e., in the event the user will be paying for a product or service with a credit card, authentication process 10 may invoke credit card verification at this point (column 11, lines 17-19)].

j. Referring to claims 32-35:

i. These claims have limitations that is similar to those of claims 23-24, 26, and 28, thus they are rejected with the same rationale applied against claims 23-24, 26, and 28 above.

k. Referring to claims 43-46, 48-50, 52-53:

i. These claims have limitations that are similar to those of claims 1-4, 6-8, and 10-11, thus they are rejected with the same rationale applied against claims 1-4, 6-8, and 10-11 above.

k. Referring to claims 71-77:

i. These claims have limitations that are similar to those of claims 29-35, thus they are rejected with the same rationale applied against claims 29-35 above.

Art Unit: 2135

l. Referring to claims 85, 89:

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

m. Referring to claim 87:

i. This claim has limitations that is similar to those of claim 71, thus it is rejected with the same rationale applied against claim 71 above.

n. Referring to claim 91:

i. This claim has limitations that is similar to those of claim 29, thus it is rejected with the same rationale applied against claim 29 above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 5, 9, 12-15, 16-20, 23-28, 36-39, 51, 54-62, 65-70, 78-79, 80-81, 86, 88, 90, and 92 are rejected under 35 U.S.C. 103(a) as being unpatentable over French et al (US 6,282,658 B2).

a. Referring to claims 9, 12-15:

i. French teaches the claimed subject matter, however, French does not precisely point out the specific information containing in the digital certificate. However, French does imply:

(1) wherein the digital certificate includes a proofing workstation validation; certificate status, which is active, hold, or revoked [**i.e., the digital certificate 902 contains information related to the issuer of the digital certificate and fingerprint data for the digital certificate (column 16, lines 12-20)]**].

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly state every detailed information within the digital certificate as shown in Figure 41 of French for authenticating the identity of network users (**column 1, lines 22-23**).

iv. The ordinary skilled person would have been motivated to:

(1) clearly state every detailed information within the digital certificate as shown in Figure 41 of French to provide an authentication system and method which preprocess information supplied by the user to check, for example, the standardization, format, validity and internal consistency of that information before comparing it to known data (**column 2, lines 26-30**).

b. Referring to claim 5:

i. French further teaches:

(1) wherein the certificate authority is a United States Postal Service digital certificate authority [**i.e., Figure 41 illustrates a digital certificate generated according to French's invention showing "This Certificate was issued by:". This is a place where the issuer's name (such as "United States Postal Service") could be included**].

c. Referring to claims 16, 19:

i. These claims have some limitations that is similar to those of claims 1-15, thus they are rejected with the same rationale applied against claims 1-15 above.

ii. In addition, French further teaches:

(1) verifying, at the proofing workstation, the identity of the user via the identification verification form with information provided by the user in person at the proofing workstation; when the identity of the user has been verified, sending by the proofing workstation an identification verification to the proofing server [**i.e. in the event the user will be paying for a product or service with a credit card, authentication process 10 may invoke credit card verification at this point. In this case, checks may be executed against a credit card database. These checks may include ensuring that the available credit line is sufficient to make the purchase, ensuring that the billing address for the credit card in the database matches the**

submitted address, and ensuring that the credit card is not stolen. Databases presenting this sort of information are commercially available (column 11, lines 17-26). In addition, referring to Figure 1, Preprocessing step 26 may thus include a set of validation checks including standard field checks, social security number validation, address validation, area code validation, and driver's license validation and other preliminary data verification (column 8, lines 50-55). Furthermore, responses, or actions, for each of the possible address-related status codes or error codes in error code matrix 156 (illustrated in Figures 9-11) are provided as output during the preprocessing step 26. The user is preferably given only one additional attempt to correct each address that has been rejected by address validation. If the address cannot be corrected after a total of two attempts, the request proceeds as designated in the response matrix 154 illustrated in Figures 9-11. The response matrix 154 may be located on authentication server 120, in authorization database 152 or elsewhere and serve to associate messages with test results and transaction records during the address portion of preprocessing step 26, concurrently with overall application processing. In other words, the response matrix 154 sends messages to client 110 based upon specific verification tests or based upon the current status of the transaction record 112. For example, the message may prompt the user to verify that data which was input is correct or a message to direct the user to call customer service for manual intervention. The response matrix 154 is preferably parameter driven, so that appropriate messages can be associated with particular events (column 10, lines 28-50)];

(2) in response to the identification verification, setting, by the proofing server, the status of the digital certificate to active [i.e., once the authentication process has been satisfied, the invention may generate a digital certificate recording authentication levels and other information related to the user. The digital certificate can then be presented in future transactions to avoid the need to re-authenticate the user for each new transaction event. (column 2, lines 62-67)]; and storing at the proofing server, the digital certificate in the electronic

Art Unit: 2135

account of the user [i.e., the biometric data may also include DNA database matching. In general, any biometric technology now existing or developed in the future may be incorporated in the invention. The biometric data may be used as input fields or records in the preprocessing, first or second authentication level stages. Alternatively, biometric data may be used as a key to unlock and release a digital certificate 902 issued to the user, to be stored on client 110 or otherwise, wherein client 110 is a client/server system (column 12, lines 56-63). Furthermore, as illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or password information to generate and store digital certificate 902 (column 16, lines 12-15)].

e. Referring to claim 17:

i. French further teaches:

(1) linking the digital certificate to a transaction on the network by the user, wherein the digital certificate can be used to authenticate the transaction [i.e., according French's invention, a user who wants to access information or process a transaction over a network is prompted to submit information to authentication process 10 through client 110. Authentication process 10 invokes the preprocessing step 26, in which the user is prompted to supply a first type of user identification information. The first type of user identification information preferably comprises wallet-type information such as name, address, phone number, social security number, driver's license number and other common personal information (column 6, lines 15-24). In addition, authentication process 10 matches, at step 32, the first type of information input by the user with information received from one or more separate data sources. Authentication process 10 also determines whether a request for information has been repeated more than a predetermined number of times at step 42. As illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or password information to generate and store digital certificate 902 (column 16, lines 12-20)].

f. Referring to claim 18:

i. French further teaches:

(1) storing a reference to the digital certificate in a certificate directory at the proofing server [i.e., as illustrated in Figures 37-40, after an indication of successful authentication the user is directed to input identification and challenge or password information to generate and store digital certificate 902. The digital certificate 902 contains a set of fields including user identification, a digital certificate serial number, an expiration period, as well as information related to the issuer of the digital certificate and fingerprint data for the digital certificate (column 16, lines 12-20)].

g. Referring to claim 20:

i. This claim has limitations that is similar to those of claim 18,

thus it is rejected with the same rationale applied against claim 18 above.

h. Referring to claim 23:

i. French further teaches:

(1) wherein the proofing workstation includes at least one of a bar code scanner, a camera, and a biometric reader (e.g., imprint peripheral) [i.e., biometric data may be employed either alone or in combination with the above preprocessing as well as subsequent authentication levels to ensure the identity of a user. That biometric data may include, for example, fingerprint information from the user, captured in analog or digital form, for instance, via an imprint peripheral connected to client 110. Biometric data may also include infrared or other digital retinal or iris scans (column 12, lines 44-55)].

i. Referring to claim 24:

i. French further teaches:

(1) wherein the identification verification is a bar code read from the identification verification form [i.e., biometric data may be employed either alone or in combination with the above preprocessing as well as subsequent authentication levels to ensure the identity of a user. That biometric data may include, for example, fingerprint information from the user, captured in

Art Unit: 2135

analog or digital form (that is a type of bar code), for instance, via an imprint peripheral (scanner is one of these peripherals) connected to client 110 (column 12, lines 44-55)].

j. Referring to claims 25-26:

i. These claims have limitations that is similar to those of claim 23, thus they are rejected with the same rationale applied against claim 23 above.

k. Referring to claim 27:

i. French further teaches:

(1) wherein the proofing server is a United States Postal Service proofing server [i.e., referring to Figure 12, element 120 could represent a United States Postal Service authentication/proofing server].

l. Referring to claim 28:

i. French further teaches:

(1) wherein the proofing workstation is a United States Postal Service proofing workstation [i.e., referring to Figure 12, element 140 could represent a United States Postal Service computer and/or workstation].

m. Referring to claim 36, 90, 92:

i. These claims have limitations that is similar to those of claim 16, thus they are rejected with the same rationale applied against claim 16 above.

n. Referring to claims 37, 39:

i. These claims have limitations that is similar to those of claim 18, thus they are rejected with the same rationale applied against claim 18 above.

o. Referring to claim 38:

i. This claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

p. Referring to claims 51, 54-57:

i. These claims have limitations that are similar to those of claims 9 and 12-15, thus they are rejected with the same rationale applied against claims 9 and 12-15 above.

q. Referring to claims 58-62, 65-70:

i. These claims have limitations that are similar to those of claims 16-20, and 23-28, thus they are rejected with the same rationale applied against claims 16-20, and 23-28 above.

r. Referring to claims 78-79:

i. These claims have limitations that are similar to those of claims 36-37, thus they are rejected with the same rationale applied against claims 36-37 above.

s. Referring to claims 80-81:

i. These claims have limitations that are similar to those of claims 15 and 20, thus they are rejected with the same rationale applied against claims 15 and 20 above.

t. Referring to claim 86, 88:

i. These claims have limitations that is similar to those of claim 58, thus they are rejected with the same rationale applied against claim 58 above.

6. Claims 21-22, 40-42, 63-64, 82-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over French et al (US 6,282,658 B2), and further in view of Messing (US 6,745,327).

a. Referring to claim 21:

i. French further teaches:

(1) sending a private key from the proofing workstation to the proofing server, when the identity of the user is verified in person **[i.e., the biometric data may be used as input fields or records in the preprocessing, first or second authentication level stages. Alternatively, biometric data may be used as a key to unlock and release a digital certificate 902 issued to the user, to be stored on client 110 or otherwise (column 12, lines 59-63)]**.

ii. Although French does not explicitly mention the use of the private key in verifying, storing or generating the digital certificate, Messing teaches:

(1) Figure 2 shows the authentication process. A user desiring to sign a document is authenticated by the certification authority computer on

Art Unit: 2135

the basis of both the certificate and the user's secret or shared secret (**column 6, lines 38-59**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have combined the teaching of Messing into French for authenticating the identity of network users (**column 1, lines 22-23**).

iv. The ordinary skilled person would have been motivated to:

(1) have combined the teaching of Messing into French to provide an authentication system and method which preprocess information supplied by the user to check, for example, the standardization, format, validity and internal consistency of that information before comparing it to known data (**column 2, lines 26-30**).

b. Referring to claim 22:

i. This claim has limitations that is similar to those of claims 21 and 13, thus it is rejected with the same rationale applied against claims 21 and 13 above.

c. Referring to claims 40-42, 82-84:

i. These claims have limitations that are similar to those of claims 21-22, and 27, thus they are rejected with the same rationale applied against claims 21-22, and 27 above.

d. Referring to claims 63-64:

i. These claims have limitations that are similar to those of claims 21-22, thus they are rejected with the same rationale applied against claims 21-22 above.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

August 11, 2006

Chankya B. - [Signature]
AU 2135